遠隔講義を想定した
IoTシステム開発演習用基盤の開発と運用

三浦　彰人

東北公益文科大学総合研究論集第42号 抜刷

2022年1月31日発行

研究論文

遠隔講義を想定した IoTシステム開発演習用基盤の開発と運用

三浦　彰人

1. はじめに

2010年代に入り、人工知能（AI）技術が急速に発達し、さまざまなICTサービスにAI技術が取り入れられるようになった。このAI技術の発達には、実社会を源とした複雑なデータ（ビッグデータ）が大量に蓄積され、現実的な時間の範囲内で利用可能となったことが大きく関係している。大量かつ多種多様な「モノ」がインターネットに接続され、それらが相互にデータをやり取りするしくみである「モノのインターネット（Internet of Things, IoT）」はその一端を担っている。これまで情報通信を担ってきたPCやサーバなどに限らず、家電製品や車、工場設備、農機具、事務機器、医療機器など、ありとあらゆる「モノ」がIoT化の対象となり始めており、総務省による情報通信白書令和3年版においても、IoTデバイスの急速な普及が取り上げられている[1)]。

これに伴い東北公益文科大学では、2020年度より酒田市委託事業として履修証明プログラム「ビッグデータ解析」[1]を開催している。この「ビッグデータ解析」では、センサデバイスを用いたデータの収集と蓄積などをテーマとした「IoTシステム開発演習」を併せて行っており、センサデバイスを接続したIoTデバイスを用いた演習を行う基盤の開発が課題となっていた。これに加え、2020年度の講義開始直前となって新型コロナウイルス感染症の影響が国内にも生じ始め、その影響が本講にも及び、教室を用いた演習が行えない可能性が高まった。そのため、急遽オンラインで演習を行える基盤とする要件を追加することとなった。

[1] 2021年度 東北公益文科大学履修証明プログラム「ビッグデータ解析」
https://www.koeki-u.ac.jp/admissions/big_data.html

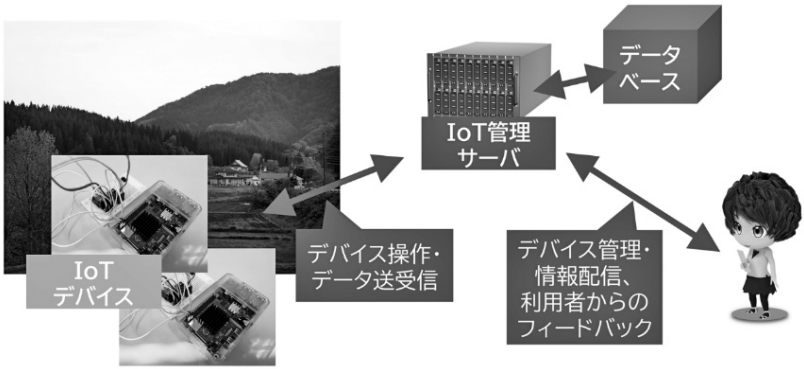

図 1 一般的なIoTシステムの構成

一般的なセンサデバイスを用いたIoTシステムの構成は図1のようになっている。利用者とサーバの間は通常のWebシステムとほとんど変わらないが、ここに多数のIoTデバイスが加わる。このIoTデバイスに付随するセンサを用いてデータの取得を行い、インターネットを経由しサーバに集積され、ビッグデータとなる。このような構成では、サーバやIoTデバイス購入と導入、電源の用意、ネットワーク環境の構築、設置環境の整備などといったイニシャルコストの他に、各IoTデバイスに光熱費や通信費といったランニングコストが発生する。通常のWebシステムと比較しより多くのデバイスを導入・管理することになるため、管理コストも増加しやすい。これら総所有コストを如何にして低く抑え、効率よく運営するかが重要となる。

また、インターネット経由で通信する以上、サイバー攻撃の対象となるリスクが常に発生する。情報処理推進機構による情報セキュリティ10大脅威2020では、組織における情報セキュリティの第8位に「IoT機器の不正利用」が挙げられている[2)]。実際に2016年には、IoT機器を対象としたマルウェア「Mirai」が猛威を振るい、Miraiに感染しボットネットに組み込まれたIoT機器による大規模なDDoS(Distributed Denial of Service)攻撃が行われた。このマルウェアは、IoT機器に組み込まれた管理用のデフォルトIDとパスワードを用いてtelnetによるログインを試行し、もし成功すればその機器を踏み台として更にターゲッ

トとなるIoT機器を探索するという比較的単純なものであったが、世界中で大きな被害（IoT機器の乗っ取り、DDoS攻撃による業務妨害）をもたらした[3]。Miraiをはじめとした機器の乗っ取りを行う攻撃においては、IoT機器の利用者はサイバー攻撃の被害者になるだけでなく、加害者に加担する事にもなりうる。従ってIoTシステムの開発においては、利用者が安全に利用しやすくなるセキュリティ設計が必要である。IoT機器におけるセキュリティ設計のガイドラインとしては、情報処理推進機構によるもの[4]やOpen Web Application Security Project（OWASP）によるもの[5]などがあり、この中のOWASP IoT 2018 Top 10は、土居らによるIoTセキュリティ教材開発[6]にも用いられている。

2. 課題

「IoT システム開発演習（以降、本演習と呼ぶ。）」の実施基盤の構築にあたり、大きな課題として次の５つが存在する。本研究では、これらの課題を解決しつつ演習の基盤を開発・運用することを目指す。

2.1. IoTデバイス管理に関する課題

IoTデバイスをはじめとする情報機器を多数の受講者に貸与し演習を行う際は、検品やセットアップ、動作検証といった事前準備にかかる時間と手間が大きくなりやすい。また、講義期間中の緊急の更新プログラムの適用作業や、講義期間終了後に返却されたIoTデバイスを初期化・更新し再設定する作業なども必要である。これらをひとつひとつ手作業で行うこと、また複雑な作業を受講者に委ねることは現実的ではないため、省力化を考慮した自動化が必要である。

2.2. IoTデバイスの可用性に関する課題

IoTデバイス開発に用いられるIoTデバイスには、主となるストレージとしてmicroSDカードなどの安価なフラッシュメモリが用いられる。フラッシュメモリは書き込み可能回数が限られており、それを超えた書き込みは行えない[7]。そのため、パッケージ更新やログの書き込みなどが大量に発生した際に故障するケースが多い。このような障害による可用性の低下は、オンライン講義では対応が後手に回り影響が大きくなりやすいため、可能な限り回避したい。

2.3. IoTデバイスのセキュリティに関する課題

本演習では、IoTデバイスにおけるセキュリティについても演習内容に含まれているが、演習内で取り上げる前の段階においても最低限のセキュリティを担保しなければならない。

2.4. コンピュータを用いた演習を含むオンライン講義における課題

オンライン講義を前提とする場合、学修に用いるネットワーク環境とPC環境によっては、受講が困難となる可能性がある。特にネットワーク環境については、ビデオ会議システムやチャットシステムの利用、Webサイトや動画の閲覧などを行っている中でIoTシステムによる通信が発生することになるため、通常より負荷が高くなりやすい。これらの配慮が必要か、また配慮が必要であればどの程度のものが必要かを調査・検討しなければならない。

2.5. 対面講義における演習と情報処理教室環境の課題

新型コロナウイルス感染症の影響の大小により、遠隔講義ではなく対面講義となる可能性も存在するため、対面講義となった場合の実施方法についても考慮が必要となる。対面講義において利用が想定される本学の情報処理教室は、画面転送方式を用いたシンクライアントとして構成されており、USBの利用には制限があるため、IoTデバイスをUSBで接続し操作する演習は行えない。そのため、対面講義の場合は受講者個人所有PCの持ち込みが前提となる。またそれに従って、本演習中はIoTデバイスに加え持ち込みPCも含めたネットワーク環境が必要となるため、受講者数×2台分の接続に耐えうる無線ネットワークを用意しなければならない。

3. 学修環境の調査

遠隔講義における演習では、受講者の自宅学修環境による影響が大きい。本講義で受講者による準備が必要となる環境は次の通りである。

- Wi-Fiによる無線通信とUSB-Serialアダプタを用いたシリアル通信ができ、遠隔講義に参加可能なPC
- インターネット上のサーバと、次のような通信ができるネットワーク環境
  - アプリケーションパッケージや更新プログラムの入手
  - IoTデータ集積サーバとのやり取り

PCについては、一般的なオンライン講義に参加できる程度を前提とするが、IoTデバイス操作の演習にシリアル通信を用いるため、貸与するUSB-Serialアダプタが利用できることも条件となる。万が一所有していない場合でも、IoTデバイス自体をPCの代替として利用することも構成によっては可能である[2]。その場合はIoTデバイス上でデスクトップ環境を動かすことになるため、デスクトップ環境を構成するアプリケーションの管理も考慮しなければならない。

またネットワーク環境については、IoTデータ集積サーバとのやり取りは必須となるため、インターネット接続は必須となる。ここでやり取りするデータとしては、各センサから収集した数十バイト程度のテキストまたはバイナリデータ、カメラを用いて撮影した数百KB程度の画像データなどが想定される。数十バイト程度のデータを毎分やり取りする程度であれば、2021年現在におけるスマートフォンのモバイル回線であっても問題にならないと考えられるが、画像データなどを扱う場合は配慮が必要となる可能性が高い。そこで、講義受講者22名に対し、受講者の自宅オンライン学修環境のうちネットワーク環境（表1）と学修用PC構成（表2）の調査を行った（回答数19）。この調査は、実際に受講した者に対して行ったものであるので、受講を希望していたが、環境

表1 オンライン学修環境のネットワーク形態

ネットワーク形態	回答数
固定回線（定額制）	13
モバイル回線（従量課金）	3
学内システムの利用（寮、学内無線LAN）	2
その他	0
インターネット接続を利用していない	1

表2 オンライン学修環境のPC構成

PCのOS	回答数
Windows 10	11
macOS	2
Linux	6
その他	0

[2] 用いるデバイスのハードウェア構成や性能による。

が整わないので受講を諦めた学生などが含まれていない点に注意が必要である。

ネットワーク環境については、おおむね定額制の固定回線が利用できるようだが、実質的に従量課金のモバイル回線のみしか利用できない受講者も僅かながら存在することが判明した。また、学修用PCのOSについては、Windows 10とmacOS、Linuxとまちまちであり、またLinuxディストリビューションやそのバージョンも多岐に渡る[3]。従って、ネットワーク環境が貧弱な受講者に対するサポートと、受講者が利用しているOSに応じたサポートが必要と考えられる。

受講者が貸与された機器を利用する機会は、講義とレポート作成、予習・復習が主となる。講義以外の学習時間は、原則として回ごとに2〜3時間程度を想定している。受講者がサポートを必要とするのは主にこの時間内であり、またこの際に貸与機器やシステムに障害が発生すると、受講や課題提出に支障が出る可能性が高い。従って、サポート体制の確立の他に、現実的な範囲で障害が発生しにくい機器やサービス、システムの選定と、障害発生時の速やかな復旧も必要である。

そこで、どのようなタイミングで貸与機器やサービスが集中的に利用されているか（どのタイミングでのサポートが必要か）を調査するため、本演習の受講者がいつレポートを作成・提出しているかを、提出締切日までの日数（図2）と提出時間帯（図3）を基準に集計した（n=275）。本演習は木曜5限（17:00〜18:45）に実施し、レポート提出締め切りは翌週火曜の23:59に設定している。

この調査により、レポートの作成と提出は主に夕方から深夜にかけて行われ、週末の休日を挟み締め切り日に提出されることが多いことが分かった。このことから、授業外学習の支援は講義時間内の他にこれら休日や深夜などの時間帯を中心としたサポートも必要と考えられる。

しかしながら、学内情報システム群の管理やレポートに関する問い合わせへの対応は教員個人が業務の片手間で行わざるを得ないのが実情であり、休日・深夜対応の恒久的な実施は現実的ではない。万が一障害が発生した場合は、翌営業日以降まで対応が遅れることも想定される。そのため、可能な限り学内情

[3] 確認できた範囲ではUbuntu、Linux Mint、Chrome OSが存在した。バージョンもまちまちである。

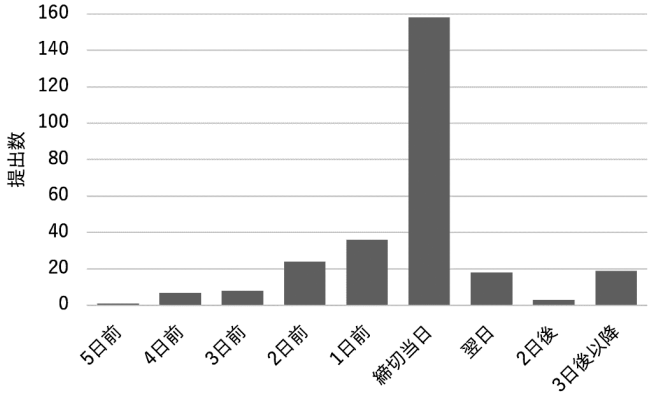

図 2 締め切り日を基準とした提出数分布

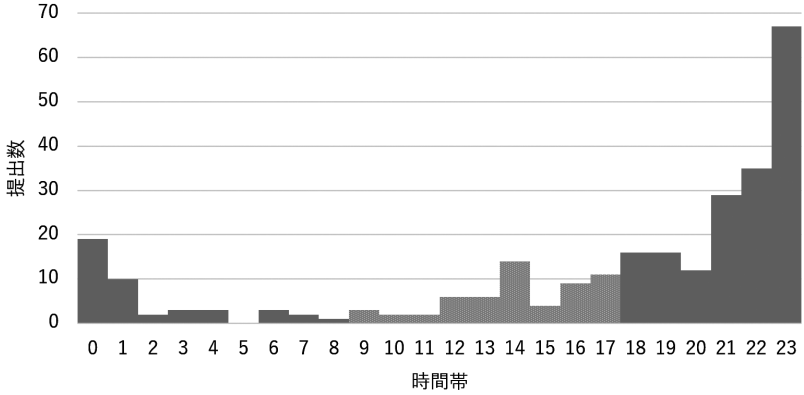

図 3 提出時間帯ごとの提出数分布

報システムに依存しない、クラウドサービス等の外部サービスや学生所有の学修環境を活用したシステム基盤構成を取る方針とする。

4. 設計と実装

本演習の2020年度の受講者数を参考に受講者数を30名と想定し、課題と調査結果を考慮しつつ設計と実装を行う。本演習の基盤は、「演習システム」、「IoTデバイス構成管理システム」、「イメージ配信システム」の3つで構成される。

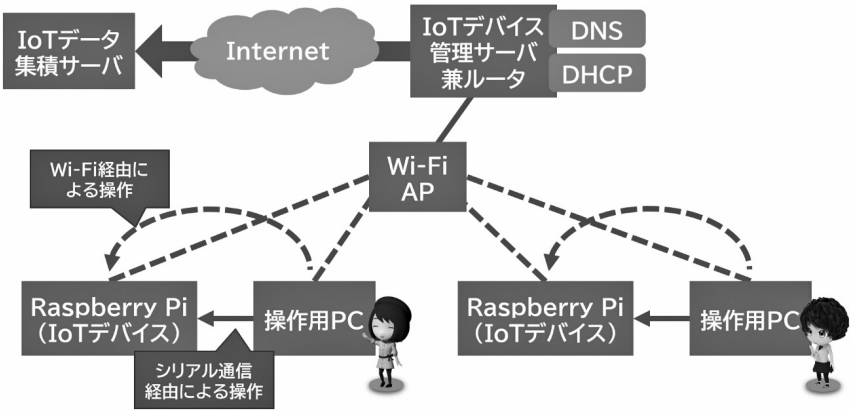

図 4 演習システムの概要

4.1. 演習システム

演習システムは、実際に本演習を行う際に用いられるシステムであり、図 4 のように構成される。受講者はIoTデバイスをWi-Fiに接続し、収集したデータを「IoTデータ集積サーバ」に送信・集積し、分析・活用するアプリケーションを開発する演習を行う。演習の際には受講者個人所有のノートPCを持ち込んでもらい、IoTデバイスにシリアルインタフェースまたはWi-Fiを経由し接続して操作する。この際にネットワーク接続とIoTデバイスの操作が円滑に行えるよう、「IoTデバイス管理サーバ」を用意し、DHCPによるIPアドレスの固定割り当てやDNSによる名前解決などをここで担当する。

IoTデータ集積サーバは、IoTデバイスからのデータを受け取り、それを分析した結果を用いてWebサービスを提供するためのものである。本サーバは、仮想専用サーバ（Virtual Private Server, VPS）提供サービスである「さくらのVPS[4]」を用いて構築する。VPSの内部は一般的なWebサービスと同様に、Linux上でWebサーバnginx[5]とRDBMSのPostgreSQL[6]、作成したWebアプリケーションの3つを置く構成となっている。IoTデバイスは、nginxを介してIoTデバイスからのデータ受信を担当するWebアプリケーションのREST

[4] さくらのVPS https://vps.sakura.ad.jp/
[5] nginx https://nginx.org/en/
[6] PostgreSQL https://www.postgresql.org/

APIを呼び、Webアプリケーションは受け取った情報をPostgreSQLに蓄積する。利用者にデータ分析を行った結果を用いたサービスを提供するWebアプリケーションは、このPostgreSQLに蓄積されたデータを用いる。

「IoTデバイス」としてはRaspberry Pi 4 model B（以降、Raspberry Pi 4と呼ぶ）を用いる。Raspberry Piは、主に教育研究用途向けに開発され、2012年より販売されている安価な小型シングルボードコンピュータである。Raspberry Pi 4 model Bは2019年に発売され、2021年現在のRaspberry Piシリーズにおいて最も性能が高いモデルである。Gigabit EthernetやWi-Fi、Bluetooth、USB3.0、GPIO、MIPI CSI-2、HDMIなどの入出力ポートが豊富に備わっており、それらに関する公式資料も多数用意してあるなど、コンピュータを用いた教育やIoTデバイス開発用として優れた特徴がある[8)]。

このRaspberry Pi 4に、Raspberry Pi用として開発されているLinuxディストリビューションであるRaspberry Pi OS（armv7h版）を導入し、講義用にカスタマイズした上で貸与する。事前にカスタマイズして配布することで、講義・授業外学習時間内における講義内容との関係が薄い作業の量と、受講者のネットワーク環境への負荷の低減を図る。Raspberry Pi OSにはデスクトップ環境を含む「with Desktop」と、デスクトップ環境を含まない最小構成の「Lite」が存在する。Raspberry Pi 4の操作形態として、一般的なPCのようにHDMIやUSBを用いてディスプレイとキーボード、マウスなどを接続した操作、Ethernet/Wi-Fiネットワーク経由での操作、シリアルインタフェース経由でのコマンド操作の3つが想定される。先述の通り講義内ではシリアルインタフェース経由とネットワーク経由での操作のみを取り扱うが、本システムでは、受講者が自宅などで別途PCを利用せずにRaspberry Pi 4にキーボードやマウス、ディスプレイを接続して演習が可能となるよう「with Desktop」をベースとし、講義でスムーズに扱えるようカスタマイズする。カスタマイズ内容は次の通りである。

- 講義で用いるソフトウェアやライブラリの追加
- 日本語ロケールへの切り替え、日本語入力の有効化
- 講義で用いるデバイスの有効化
- 最低限のネットワーク設定

• ファイアウォールやアクセス権限など、セキュリティに関する設定
• IoTデバイス構成管理システム利用の際に必要となるスクリプトの追加

講義内容との整合性と汎用性の維持、メンテナンスコスト低減を考慮し、必要最小限の追加・変更に留める。またセキュリティに関しては、セキュリティに関する演習を行う前であってもネットワーク経由での不正アクセスに遭いにくくなるよう、OWASP IoT Top 10[5] などを参考にしつつファイアウォールやリモートログインサービスの設定などを行う。

このような情報機器を教育目的として貸与する際に一般に課題となるのは、受講者が行使できる権限の制限である。高い権限を与えれば、誤操作や悪意のある操作による障害や不正利用が発生する可能性が高まるが、低い権限では実行できることの幅が狭まり、それらを学ぶ機会が失われる。本講義にはデバイス操作を行うプログラムの作成やOS環境の管理といった高い権限を必要とする内容が含まれるため、Raspberry Pi 4を受講者が利用する際は、通常時は一般ユーザ権限で操作し、必要に応じて管理者権限を行使できるよう構成する。その分、回収後の再構成や障害発生時の復旧の容易さが重要となってくる。

本演習で受講者に貸与するハードウェア類は、次の一式を30組用意する。
• Raspberry Pi 4 model B本体（メモリ8GB）
• microSDXCカード（64GB, A2, Read: 160MB/s, Write: 60MB/s）
  Raspberry Pi 4の主要ストレージとなるmicroSDXCカード。この中にルートファイルシステムが置かれ、ほぼ常になんらかのデータが読み書きされる状態となるため、書き込み耐久性能（Total Bytes Written, TBW）が重要である[7]。速度についてはRaspberry Pi 4側インタフェースの上限があるため、高速なmicroSDXCカードを用いてもおおよそ40〜50MB/s程度が最大転送速度となる。
• USB-Serial変換アダプタ（3.3V）
  PCからRaspberry Pi 4のシリアルインタフェースに接続する。本講義内では主にこのシリアルインタフェースまたはEthernet/Wi-Fiを経由して

[7] 高い書き込み耐久性能や広い動作温度範囲を持つ産業用microSDXCカードを用いることも可能であるが、高コストとなる。

Raspberry Pi 4を操作することを前提とする。

- 温湿度センサ、ジャンパワイヤ（DHT11, GPIOに接続）
  センサデータの収集を行う演習に用いる。Pythonなどで記述された専用ライブラリを用いてデータを取得できる。
- カメラ、カメラケーブル（MIPI CSI-2[8]接続）
  センサデータの収集を行う演習に用いる。V4L2 API[9]やそれを操作するアプリケーションを用いて画像や動画を取得できる。
- Raspberry Pi 4用ケース
  Raspberry Pi 4本体を保護する。本体のみの場合は基盤が剥き出しの状態であり、静電気や衝撃などで故障する可能性が高くなるため必須となる。
- Raspberry Pi 4 SoC用ヒートシンク
  Raspberry Pi 4のSoCは高温になると自動的にクロック周波数を落とし、熱による破損を防ぐサーマルスロットリング機能があり、これが働くと性能が大きく低下する[9)]。この問題を可能な限り低減するため、排熱効率を向上させるヒートシンクを用意する。
- ACアダプタ（5V 3A, USB Type-C）
  Raspberry Pi 4の電源用ACアダプタ。
- microHDMI-HDMIケーブル
  Raspberry Pi 4とディスプレイを接続するためのもの。講義では直接用いないが、受講者の自宅での使用を想定した。

4.2. IoTデバイス構成管理システム

演習システムで用いるRaspberry Pi OSをカスタマイズする際に大きな課題となるのは、その構成を如何にして全てのRaspberry Pi 4に適用するかという点である。手動で行うことも不可能ではないが、台数が増えれば増えるほど当然その手間は大きくなる。また、貸与後の構成管理は原則として指導を行った上ではあるものの受講者に委ねられる形となるため、一定の状態に保つことは非常に困難である。

---

[8] MIPI Camera Serial Interface 2 https://www.mipi.org/specifications/csi-2

[9] The Linux Kernel user-space API guide - Video for Linux API https://www.kernel.org/doc/html/v5.15/userspace-api/media/v4l/v4l2.html

そこで本基盤では、構成管理ツールAnsible[10]を基盤とした構成管理システムを構築する。Ansibleを実行すると、管理者が記述した構成ファイル（Playbook）に従った操作が機器上で行われ、Playbookに記述された一定の状態に保たれる。これにより、パッケージの追加・更新や設定ファイルの記述など、これまで手動で行ってきた定型作業を一括して自動化できる。同様のツールにChef[11]などがあるが、Ansibleはプログラミング言語Pythonが利用できる環境であれば動作する特徴がある。PythonはRaspberry Pi OSの基本構成に含まれるため、Ansibleを採用した。AnsibleのPlaybookの管理は、ソースコードホスティングサービスであるGitHub[12]の公開リポジトリを用いて行う。

この構成管理システムは、貸与前の初期設定と、貸与後の更新に用いられる。初期設定の際は、SDカードに何も書き込まれていない状態であるため、ベースとなるRaspberry Pi OSイメージの書き込みと、ホスト名などの本体固有の設定、MACアドレスの収集などが必要となる。ベースイメージは、ベースイメージ作成用Raspberry Pi 4上でAnsibleを用いて作成する。作成されたイメージは、iSCSIを通じてイメージ配信システム内のストレージに記録される（図5）。

貸与後の構成更新は、受講者の行動の妨げとならないよう、受講者自らが手動で構成管理システムを利用できるようにする。バックグラウンドでの強制自

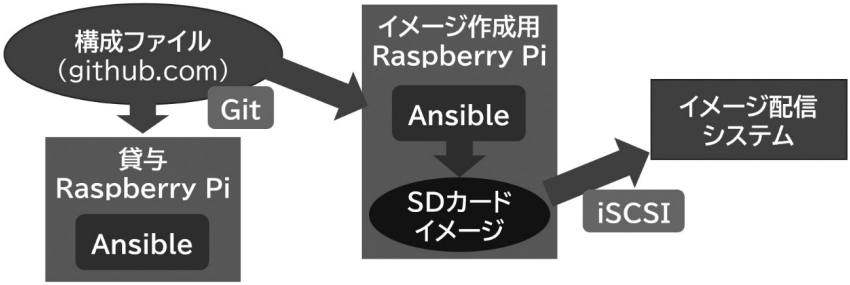

図5 IoTデバイス構成管理システムの概要

[10] Ansible is Simple IT Automation https://www.ansible.com/
[11] Chef Software DevOps Automation Solutions https://www.chef.io/
[12] GitHub: Where the world builds software https://github.com/

動更新とした場合、中途半端な状態での電源断などが発生する可能性もあり障害の原因になりうるため、本システムでは行わない。構成管理システムを利用する際は、それが適切に実行されているか管理者が確認できるよう、実行ログの送信が行われる。

4.3. イメージ配信システム

IoTデバイス構成管理システムを用いて作成したベースイメージのmicroSDXCカードへの書き込みを行う手法として、下記のふたつの形態が考えられる。

1. イメージを丸ごとそのままmicroSDXCカードに書き込む。
2. イメージ内のファイルとmicroSDXCカード上のファイルについて、差異があるもののみmicroSDXCカードに書き込む。

単純な処理で行えるのは1の手法であるが、イメージ全体を書き込むため書き込み量が多くなり、作業時間の増大とmicroSDXCカード寿命の短縮に繋がる。よって本基盤では差分を書き込む手法を取った。また、このような作業を複数台の機器に対し手作業で行うと、作業漏れや不注意による機器の損傷が発生しやすくなる。特にRaspberry Pi 4のmicroSDカードスロットは、利用する本体ケースによってはmicroSDXCカードの抜き差しがしにくく[13]、スロットやカードを壊しかねないため、抜き差しを伴う作業は極力減らしたい。そのため本基盤では、特定のネットワークに接続するだけで自動的に初期化・更新が行われる「イメージ配信システム」を構築し、複数台を対象とした一括展開・更新を実現する。イメージ配信システムでは、Raspberry Pi 4のネットワークブート機能を活用し、自動的に構成管理された演習用IoTデバイスイメージの書き込み・更新を行う。

まずRaspberry Pi 4のEEPROM内ブートローダイメージをカスタマイズし、ネットワークブートを最優先にする[10)]。この作業のみ自動化が困難であるため、事前に手作業にて行う。このEEPROMイメージを書き込まれたRaspberry Pi 4は、ネットワークブート環境が用意された有線ネットワークに接続し電源を

[13] メーカー公称10000回の抜き差しが可能となっている。しかし、Push-Pull型スロットであるため抜く際に指で挟み込む必要があり、その際ケースに指が干渉しうまく取り出せず強い力が掛かり、指先を負傷することがあった。

入れた際にネットワークブートするようになる。もしネットワークブート環境が無いネットワークに接続した場合は、通常通りUSBストレージもしくはmicroSDXCカードからのブートを試みる。ネットワークブートは、x86コンピュータとほぼ同様[14]にDHCPとTFTPによって、ブートに必要なファイルを取得する。

Raspberry Pi 4のブートに必要なファイルは、Raspberry Pi用ファームウェアとLinuxカーネルイメージである。これにイメージ展開用にカスタマイズしたinitramfsイメージを加え起動時に実行されるようにすることで、ネットワークに接続するだけで自動的にインストール・更新されるシステムを実現する。このinitramfs内では、次の処理が行われる（図 6）。

- DHCPによるIPアドレスの再割り当て
- microSDXCカードの初期化
  （本システムのイメージが書き込まれていない場合のみ）
- パーティションテーブルとファイルシステムの作成
  （本システムのイメージが書き込まれていない場合のみ）
- rsync[15]によるSDカードイメージとの同期

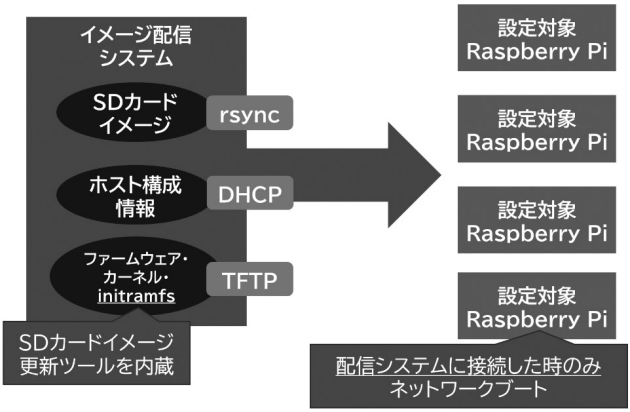

図 6 イメージ配信システムの概要

[14] DHCPサーバで発信しなければならない情報がx86 PCとRaspberry Pi 4では若干異なり、Raspberry Pi 4の場合はvendor-class-identifierとvendor-encapsulated-optionsの設定が必須である。

[15] rsync https://rsync.samba.org/

• デバイス固有の設定（ホスト名など）

これらの処理により、Raspberry Pi 4上の環境が最新のものと同期される。

イメージ配信システムによるイメージの展開は、本システムが存在するネットワークにネットワークブートを有効にしたRaspberry Pi 4を接続し電源を入れるだけで自動実行される。そのため、本システムのみ別途隔離したネットワークを用意し、Raspberry Pi 4の初期化や複数台まとめてのイメージ更新が必要な時のみ利用する形を取った。

6. 運用と評価

2021年4月の講義開始に伴って本基盤の運用を開始し、受講者へのRaspberry Pi 4の貸与を行った。受講者数は21名で、講義形式は対面となった。本基盤の運用フローを図7に示す。

6.1. サポート体制とその評価

レポート提出や問い合わせ対応の窓口、本演習内で用いるファイルの共有などを、本学が契約し受講者に割り当てているOffice365 A1のMicrosoft Teams[16]に一本化し、次の点について改善を試みた。

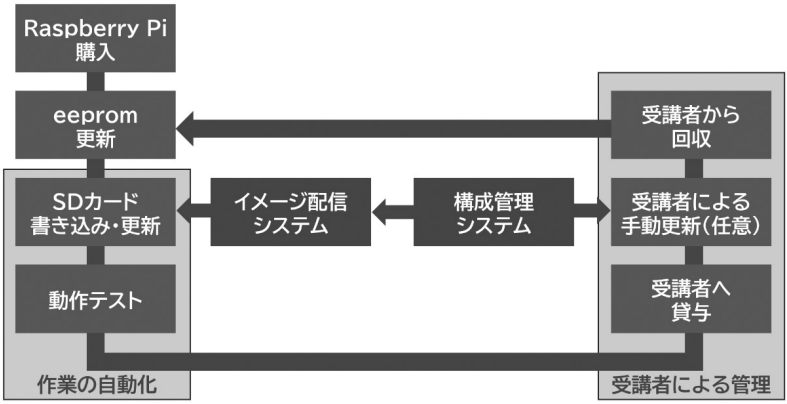

図7 本基盤の運用フロー

[16] Microsoft Teams https://www.microsoft.com/ja-jp/microsoft-teams

- チーム内公開チャネルを用いた質問の可視化
  - 受講者間での教え合いの促進と可視化
  - 効果的な質問手法の習得
- 受講者・教員の負担軽減
  - 非常時の遠隔・対面切り替えの円滑な移行
  - 各サービス・機能のシームレスな利用

2021年度の運用においては、受講者・教員の負担軽減については一定の改善が見られた。一方、チーム内公開チャネルを用いた質問の可視化については、受講者が質問チャネルを用いずに、ダイレクトメッセージやメールなどによって質問を行いがちであるといった課題が生じた。これに対して「公開チャネルにおいて積極的な質問や互助的な活動を行った受講者は、その活動についても評価する」といった対応を行ったところ、演習の後半では公開チャネルの活性化が見られた。

6.2. 受講者による評価

受講者による2021年度前期講義終了後の授業アンケートにおいて、講義時間が超過しがちであった点について複数の指摘を受けた。これは、受講者個人所有の持ち込みPCの状態が多様であり、機器の接続や設定などの作業について想定以上に手間取った事が要因として考えられる。

特に、USB-Serial変換アダプタ利用時の環境による差異や、MacBookにおけるUSBポートの少なさ、Chrome OSの機能制限などに起因する問題への対策に苦慮した。USB-Serial変換アダプタの問題は、特定のUSB-Serial変換モジュール（FT232）とGNU UUCP[17]のcuコマンドとの組み合わせでのみ発生し、入出力が正常に行われなくなるというものであった。また、演習中にWi-Fiの接続が不安定になる事態も度々発生した。演習システムの構成の都合により独自のWi-Fiアクセスポイントを1台用意し、既存設備との干渉なども考慮しつつ設置したが、そのアクセスポイントがIEEE802.11aと11nまでしか対応していなかった[18]上、そこに全員が持ち込みノートPCとRaspberry Pi 4を接続したことにより、アクセスポイントの性能限界を超えたためと思われる。

[17] GNU UUCP https://directory.fsf.org/wiki/Uucp
[18] Raspberry Pi 4は後継のIEEE802.11acに対応している。

持ち込みPCの環境による差異や演習環境の不備のような講義内容の本質とは離れた要因により講義時間が圧迫される状態は避けるべきであり、学修用PCの標準化や演習環境の更なる整備・更新といった対策が必要と考える。

6.3. 障害の発生と対応

運用期間中の障害は1件発生し、原因はmicroSDXCカードの故障によりデータの読み書きができなくなるというものであった。おそらくフラッシュメモリの書き込み限界を超えたか、熱によるものと思われる。障害発生日は8月で、作業を行っていた教室の気温は30℃前後となっていた。それに加え、パッケージ管理システムに関する操作を行っていたため、microSDXCカードに対し大量の読み書きが発生し、それに伴う発熱でかなりの高温になっていた可能性がある。本件については、予備のmicroSDXCカードへの置き換えとイメージ書き込み、受講者立ち合いの元での初回設定確認を行い、おおよそ1時間程度で復旧が完了した。

破損したmicroSDXCカードはOSで認識できるブロックデバイスサイズが数百KBとなるなど、ほぼ完全に読み取れない状態となっており、SDカードに記録されていた全てのデータが失われてしまった。幸いにもレポートなどの重要なデータは持ち込みPC側に記録されていたようだが、クラウドストレージを用いたバックアップなど、単一障害点を作りこまない手法に関する指導も必要と考えられる。

7. 考察

7.1. ネットワークブートにおけるセキュリティ上の問題

イメージ配信システムの利用を想定し、Raspberry Pi 4のブート時におけるネットワークブートの優先度を高めているが、この構成ではセキュリティ上のリスクが大きい。例として、マルウェアを含むファームウェア群を仕込んだ偽のDHCPサーバとTFTPサーバが存在する有線ネットワークにRaspberry Pi 4を接続してしまった場合、そのマルウェアが何の確認もなしに実行されてしまう（図8）。ネットワークブートにおける不正なファームウェア対策としては、EEPROM内ブートローダにおいてファームウェアやカーネルのデジタル署名を確認し、承認されたものだけを実行するSecure Boot[11]に類する機構の実装

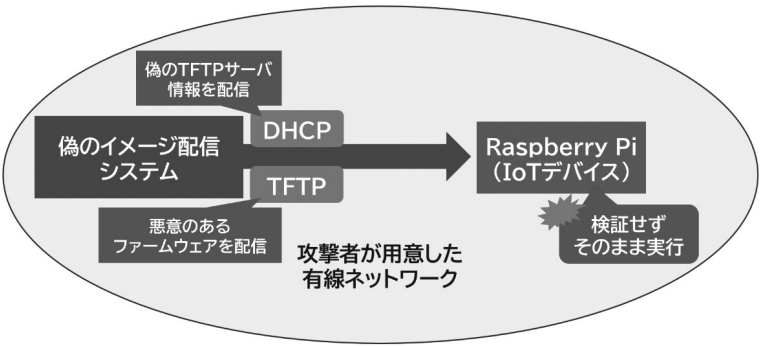

図 8 偽のイメージ配信システムによるマルウェアの実行

が必要であるが、残念ながら2021年11月現在EEPROM内ブートローダのソースコードは公開されていないため、それに類する機能を実装することは現実的ではない。

また、ネットワークブートは有線LAN経由でしか行えないため、都度ケーブルの抜き差しが必要で手間が掛かる。キッティング作業中は、多数の端末を同時に接続して作業を行うため、ケーブルなどの取り回しづらさは作業ミスの要因にもなりうる。

これらの問題を解決する現実的な手法として、USBブートの優先度を上げ、更新作業専用USBメモリを用意し、そのUSBメモリを挿して電源を入れた時のみ自動展開・更新が行われるようなシステムに作り替えるといったものが考えられる。この手法では、無線LAN経由での展開・更新やネットワーク経由でのマルウェア実行の問題を解決できるが、並列して展開作業を行う分のUSBメモリの用意が必要となる。

7.2. 機器の構成や稼働状態の把握

貸与後の機器の状態は、受講者が構成管理システムを利用し構成の更新を行った際のみログ送信が行われ管理者の元に届く。そのため更新が行われなかった場合、管理者は構成の更新が行われていないことしか認知できない。また、ログはプレーンテキストの形で収集されるため、管理者はそれを目的に応

じて都度分析しなければならず手間が大きい。そのため、Zabbix[19]のようなデバイス・ネットワーク管理ツールの導入の検討が必要である。管理ツール導入の際は、受講者のプライバシーを考慮し、演習の目的外の情報を収集しない慎重な設計が求められる。

8. おわりに

本研究では、遠隔講義を想定したIoTシステム開発演習基盤の開発と運用、評価を行った。本研究の成果は、2021年度の履修証明プログラム「ビッグデータ解析」で実際に用いられ、来年度以降も利用と改善を継続する予定である。2021年度の運用では、環境やサポート体制、指導内容の改善、イメージ配信システムのセキュリティ上の問題や、貸与中の機器構成管理、貸与前・回収後のメンテナンスコストの低減といった点について課題が残された。今後はこれらの課題の解決を試みたい。

参考文献

1）総務省. 情報通信白書令和3年版 第1部 特集 デジタルで支える暮らしと経済. 2021年7月30日.
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/html/nd105220.html. 2021年11月24日.

2）独立行政法人情報処理推進機構. 情報セキュリティ10大脅威2020. 2021年5月26日.
https://www.ipa.go.jp/security/vuln/10threats2020.html. 2021年11月9日.

3）辻宏郷. 顕在化したIoTのセキュリティ脅威とその対策. 2017.
https://www.ipa.go.jp/files/000059579.pdf. 2021年11月9日.

4）独立行政法人情報処理推進機構 セキュリティセンター. “IoT開発におけるセキュリティ設計の手引き.” 2021.
https://www.ipa.go.jp/files/000052459.pdf.

5）Open Web Application Security Project. OWASP Internet of Things

[19] Zabbix :: The Enterprise-Class Open-Source Network Monitoring Solution https://www.zabbix.com/jp

Project. 2018.
https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project. 2021年11月8日.
6）土居茂雄 , 向平卓矢. “IoTセキュリティ教材の研究開発と評価.” 2020. 工学教育　2020 年 68 巻 3 号 p. 3_46-3_51.
7）Cai, Yu et al. “Error patterns in MLC NAND flash memory: Measurement, characterization, and analysis.” 2012 Design, Automation & Test in Europe Conference & Exhibition (DATE) (2012): 521-526.
8）The Raspberry Pi Foundation. Raspberry Pi 4 Tech Specs. 2019年6月24日.
https://www.raspberrypi.com/products/raspberry-pi-4-model-b/specifications/. 2021年11月8日.
9）Alex Bate. Thermal testing Raspberry Pi 4. 2019年11月28日.
https://www.raspberrypi.com/news/thermal-testing-raspberry-pi-4/. 2021年4月30日.
10）The Raspberry Pi Foundation. Raspberry Pi Documentation - Raspberry Pi 4 Boot EEPROM. 2021年11月10日.
https://www.raspberrypi.com/documentation/computers/raspberry-pi.html#raspberry-pi-4-boot-eeprom. 2021年11月26日.
11）Wilkins, Richard, and Brian Richardson. “UEFI secure boot in modern computer security solutions.” *UEFI forum*. 2013.